What is claimed is:

1. A method of encrypting and decrypting an electronic file on a web-based computer system, comprising:

receiving, by a computer system, an electronic data file, wherein the computer system includes a memory subsystem and a plurality of memory locations;

encrypting the data file in the memory subsystem;

storing the encrypted data file in one or more of the plurality of memory locations;

retrieving the encrypted data file from the one or more memory locations;

decrypting the encrypted data file in the memory subsystem; and

displaying the decrypted data file on a web browser.

2. The method of claim 1 further comprising, prior to the receiving step:

receiving a username and a password from an external user device; and

verifying the username and password correspond to a pre-defined user having access to the computer system.

3. The method of claim 1 further comprising, between the storing step and the retrieving step:

retrieving the encrypted data file from the one or more memory locations;

analyzing the encrypted data file;

modifying the analyzed data file; and

storing the modified data file in the one or more memory locations.

4. The method of claim 1 wherein the receiving step is performed using a SSL/HTTPS protocol.

5. The method of claim 1 wherein the displaying step is performed using a SSL/HTTPS protocol.

6. The method of claim 1 wherein the memory subsystem includes random access memory.

7. A method of encrypting and decrypting an electronic data file on a web-based computer system, comprising:

receiving, by a web server, an electronic data file, wherein the web server includes a memory subsystem;

encrypting the data file in the memory subsystem;

transmitting the encrypted data file to a file server having a plurality of memory locations;

storing the encrypted data file in one or more of the plurality of memory locations;

retrieving the encrypted data file from the one or more memory locations;

transmitting the encrypted data file to the web server;

decrypting the encrypted data file in the memory subsystem; and

displaying the decrypted data file on a web browser.

8. The method of claim 7 further comprising, prior to the receiving step:

receiving, by the web server, a username and a password from an external user device; and

verifying, by the web server, the username and password correspond to a pre-defined user having access to the computer system.

9. The method of claim 7 further comprising, between the storing step and the retrieving step:

retrieving the encrypted data file from the one or more memory locations;

analyzing the encrypted data file;

modifying the analyzed data file; and

storing the modified data file in the one or more memory locations.

10. The method of claim 7 wherein the receiving step is performed using a SSL/HTTPS protocol.

11. The method of claim 7 wherein the displaying step is performed using a SSL/HTTPS protocol.

12. The method of claim 7 wherein the memory subsystem includes random access memory.

13. The method of claim 7 further comprising, between the storing step and the retrieving step:

retrieving the encrypted data file from the one or more memory locations;

transmitting the encrypted data file to a back-end data processing server;

analyzing, by the back-end data processing server, the encrypted data file;

modifying, by the back-end data processing server, the analyzed data file;

transmitting the modified data file to the file server; and

storing the modified data file in the one or more memory locations.

14. A system for encrypting and decrypting an electronic data file, comprising:

a web server for encrypting a data file and decrypting an encrypted data file, the web server having a memory subsystem;

a file server, electrically connected to the web server, for storing the encrypted data file, the file server having a plurality of memory locations; and

a back-end data processing server, electrically connected to the file server, for modifying the encrypted data file,

wherein the web server includes a computer process comprising:

receiving the data file from an external user device,

encrypting the data file in the memory subsystem, and

transmitting the encrypted data file to the file server,

wherein the file server includes a computer process comprising:

receiving the encrypted data file from the web server,

storing the encrypted data file in one or more of a plurality of memory locations,

retrieving the encrypted data file from the one or more memory locations, and

transmitting the encrypted data file to the back-end data processing server,

wherein the back-end data processing server includes a computer process comprising:

receiving the encrypted data file from the file server,

analyzing the encrypted data file,

modifying the analyzed data file, and

transmitting the modified data file to the file server.

15. The system of claim 14 wherein the computer process of the file server further comprises:

receiving the modified data file from the back-end data processing server;

storing the modified data file in the one or more memory locations;

retrieving the modified data file from the one or more memory locations; and

transmitting the modified data file to the web server.

16. The system of claim 15 wherein the computer process of the web server further comprises:

receiving the modified data file from the file server;

decrypting the modified data file in the memory subsystem; and

displaying the decrypted data file on a web browser.

17. A system for encrypting and decrypting an electronic data file, comprising:

a web server for encrypting a data file and decrypting an encrypted data file, the web server having a memory subsystem; and

a file server electrically connected to the web server, for storing the encrypted data file, the file server having a plurality of memory locations

wherein the web server includes a computer process comprising:

receiving the data file from an external user device,

encrypting the data file in the memory subsystem, and

transmitting the encrypted data file to the file server,

wherein the file server includes a computer process comprising:

receiving the encrypted data file from the web server,

storing the encrypted data file in one or more of the plurality of memory locations,

retrieving the encrypted data file from the one or more memory locations, and

transmitting the encrypted data file to the web server.

18. The system of claim 17 wherein the computer process of the web server further comprises:

receiving the encrypted data file from the file server;

decrypting the encrypted data file in the memory subsystem; and

displaying the decrypted data file on a web browser.

19. The system of claim 17 wherein the computer process of the file server further comprises, between the storing step and the retrieving step:

retrieving the encrypted data file from the one or more memory locations;

analyzing the encrypted data file;

modifying the analyzed data file; and

storing the modified data file in the one or more memory locations.

20. A system for encrypting and decrypting an electronic data file, comprising a computer system including:

a memory subsystem;

a plurality of memory locations; and

a computer process comprising:

receiving a data file from an external user device,

encrypting the data file in a memory subsystem,

storing the encrypted data file in one or more of a plurality of memory locations,

retrieving the encrypted data file from the one or more memory locations,

decrypting the encrypted data file in the memory subsystem, and

displaying the decrypted data file on a web browser.

21. The system of claim 20 wherein the computer process further comprises, between the storing step and the retrieving step:

retrieving the encrypted data file from the one or more memory locations;

analyzing the encrypted data file;

modifying the analyzed data file; and

storing the modified data file in the one or more memory locations.